REMARKS

Claims 1-86 were presented for examination and were rejected. Applicant is hereby amending claims 1, 6, 7, 12-14, 18, 20-24, 26, 30, 31, 34-37, 41, 50, 51, 54, 65-67, 69, 72, 73, and 84-86; and canceling claims 15-17. Support for all amendments is found in the application as originally filed. Reconsideration of this application as amended, and allowance of all claims remaining herein, claims 1-14 and 18-86 as amended, are hereby respectfully requested.

In numbered paragraph 11 of his Office Action Summary, the Examiner indicated that he approved the proposed drawing correction filed on November 7, 2005 as part of Amendment C. The Examiner requested that corrected drawings now be submitted to the USPTO. Applicant has in fact submitted a replacement set of 12 sheets of formal drawings on July 24, 2006. Applicant is proposing additional drawing corrections and amendments at this time as follows:

Applicant hereby amends Figures 5, 6, 7, 11 and 12 as follows:

The version of Figure 5 that was submitted to the USPTO on July 24, 2006 was a landscape-mode drawing that inadvertently printed backwards. That oversight is being corrected herein.

In Figure 6, add the number "110" to the top box; correct the designation of TBV DATA to be item 232 (as supported by page 6 lines 21-22 of the specification, and by Figures 7 and 11); and label BANK INTERFACE with numeral 222.

In Figure 7, add the numeral "110" to the top box.

In Figure 11, add the numeral "110" to the top box; and add the numeral 222 to BANK INTERFACE.

In Figure 12, add the numeral "110" to the top box; correct TBY to TBV in item 219RP (as correctly shown in Figure 4); and add the label 222 to BANK INTERFACE.

Corrected Figures 5, 6, 7, 11, and 12, with the amendments shown in red pen, are enclosed herewith as an appendix A to this Amendment D.

In his third paragraph, the Examiner rejected claims 1-17 under 35 U.S.C. §103(a) as being unpatentable over Orrin in view of Shear. Applicant is hereby amending independent claim 1 (the only independent claim in this set of rejected claims) and dependent claims 6, 7, and

12-14; and canceling claims 15-17 to highlight novel aspects of his invention. As amended, Applicant's claims are patentably distinct over the cited references for, inter alia, the following reasons:

1. There is no mention in either Orrin or Shear of executable Web browser software. On the other hand, all of Applicant's claims are directed to a method for verifying the trustworthiness of executable Web browser software, as recited in claim 1.

2. Orrin is remote, because Orrin does not authenticate anything that is executable. The only thing that Orrin executes is non-executable data. On the other hand, Applicant's claims are directed to verifying the trustworthiness of executable Web browser software, as recited in claim 1. Thus, Applicant traverses the statements made by the Examiner in paragraphs 2.2 and 3.2 of his Office Action that Orrin verifies the trustworthiness of a browser. For example, in his paragraph 2.2, the Examiner cites Orrin's paragraph 39 for this proposition. However, Orrin's paragraph 39 makes it clear that it is content (data), not executable browser software, that is authenticated. In paragraph 39, Orrin states: "In step 246, obligor 102 performs a signing function on the content... many internet browsers have signature functions as built-in features... The resulting combination of content 212, timestamp 214, and obligor's signature 216 forms signed content 210. Signed content 210 may then be sent to trusted server 100, for example, using an HTTP post operation." (emphasis added)

3. In view of what we state in paragraphs 1 and 2 above, the recitation in claim 1 of "a second digital signature serving to verify the trustworthiness of the executable browser itself" is not and cannot be suggested by the two cited references, whether taken alone or in combination.

4. In Applicant's claims, authenticating the second digital signature, which vouchsafes the executable Web browser software, occurs subsequent to the browser having signed the electronic document. This is now crystal clear in view of the words "in the following order" that Applicant is adding to claim 1 in this Amendment D.

In Shear, on the other hand, the comparison of hashes of the executable load module is performed before the executable load module executes. To verify the trustworthiness of the load module after its execution would be contrary to the purpose of Shear, which is to validate the trustworthiness of the load module prior to its running in a protected processing environment. Such a system is used to insure that the load module has not been tampered with prior to its

operation, in order to avoid executing a compromised program. Applicant's invention is not concerned with the validity of an executable program to be run in the future (such as Shear's load module). Rather, Applicant's invention is concerned with determining the validity of a digitally signed document by ensuring the validity of the signature and the trustworthiness of the browser that digitally signed the document in the past.

5. Neither reference suggests claim 1's recitation of "...the first digital signature includes as an attribute a second digital signature ..." Applicant's specification at page 10, lines 1-20, in conjunction with his Figure 8, makes clear that "attribute" means "one of the components over which the first digital signature is performed".

Claims 2-14 depend upon independent claim 1, and therefore the patentability of these dependent claims flows from the patentability of claim 1.

Further with respect to claim 7, the "attribute" recitation of claim 7 is not suggested by the prior art, whether taken alone or in combination. Claim 7 tracks the bottom of the three embodiments illustrated in Figure 8.

Further with respect to claim 12, the "attribute" recitation of claim 12 is not suggested by the prior art, whether taken alone or in combination. The embodiment recited in claim 12 is illustrated as the middle and bottom embodiments of Figure 8.

For the above reasons, the Examiner is requested to withdraw his rejection of claims 1-17; and to allow claims 1-14 as amended.

In his fourth paragraph, the Examiner rejected claims 18-86 under 35 U.S.C. §103(a) as being unpatentable over Shear in view of Sudia.

In this rejected claim set, the independent claims are claims 18, 35, 50, and 68.

Applicant is hereby amending claims 18, 20-24, 26, 30, 31, 34-37, 41, 50, 51, 54, 65-67, 69, 72, 73, and 84-86 to more particularly highlight novel aspects of his invention. As amended, claims 18-86 are patentable for, inter alia, the following reasons:

Independent claims 18 and 35 are directed to verifying the trustworthiness of an executable Web browser. Shear does not even mention Web browsers. Sudia discusses a "browser" doing a vague "certificate handshake" with a web server (paragraphs 0401 through 0434), but Sudia does not suggest verification of the executable Web browser code itself, which

is the subject matter of Applicant's claims. Furthermore, Sudia does not suggest taking the hash values that are recited in Applicant's claims.

Additionally, the only one of these references that treats the authentication of executable code, Shear, does not suggest the recitation of claims 18 and 35 that the determination of the trustworthiness of the executable Web browser is performed subsequent to the browser having executed (by virtue of its having digitally signed an electronic document).

In Shear, on the other hand, the comparison of hashes of the executable load module is performed before the executable load module executes. To verify the trustworthiness of the load module after its execution would be contrary to the purpose of Shear, which is to validate the trustworthiness of the load module prior to its running in a protected processing environment. Such a system is used to insure that the load module has not been tampered with prior to its operation, in order to avoid executing a compromised program. Applicant's invention is not concerned with the validity of an executable program to be run in the future (such as Shear's load module). Rather, Applicant's invention is concerned with determining the validity of a digitally signed document by ensuring the validity of the signature and the trustworthiness of the browser that digitally signed the document in the past.

Dependent claims 19-34 and 36-49 depend upon independent claims 18 and 35, respectively. Therefore, the patentability of claims 19-34 and 36-49 flows from the patentability of claims 18 and 35.

Further with respect to dependent claims 22, 23, 39, and 40, neither Shear nor Sudia suggests the "unknown" status of a Web browser as recited in said claims.

Further with respect to dependent claim 24, neither Shear nor Sudia suggests the step of receiving from a requestor a request to determine the trustworthiness of a Web browser module, the request including a second set of hashes, as recited in claim 24.

Further with respect to dependent claims 46-49, neither Shear nor Sudia suggests the first customer, second customer, transaction, buyer relationship, or seller relationship recited in said claims.

Independent claims 50 and 68 recite a four-corner trust model comprising a root entity, a first participant, a second participant, a first customer of the first participant, and a second

customer of the second participant. The two cited references are remote, because they neither mention nor suggest these five recited entities.

Also, all of claims 50-86 recite that the second set of hashes is transmitted by the first customer to the second customer, using a network connection. Neither Shear nor Sudia suggests transmitting hashes anywhere. Shear's hash comparisons are performed at the same microprocessor; Sudia does not use hashes to authenticate code.

Additionally, the references do not suggest the set of hashes recited in all of claims 50-86. Shear sometimes performs several different verifications on the same load module, but for each verification of an executable load module, Shear takes just one hash.

Furthermore, the references do not suggest the trusted verifier module recited in claims 50 and 68; or the detailed generating, transmitting, forwarding, and determining steps recited in claim 50; or the corresponding "means for" elements recited in claim 68.

Claims 51-67 and 69-86 depend upon independent claims 50 and 68, respectively. Therefore, the patentability of claims 51-67 and 69-86 flows from the patentability of claims 50 and 68.

Further with respect to dependent claims 53, 56, 71, and 75, neither Shear nor Sudia suggests the "unknown" browser status recited in these claims.

Further with respect to dependent claims 57, 58, 59, 76, 77, and 78, neither Shear nor Sudia suggests the transaction recited in these claims.

Further with respect to dependent claims 60 and 79, neither Shear nor Sudia suggests the root entity operating rules recited in these claims.

Further with respect to dependent claims 63, 64, 82, and 83, neither Shear nor Sudia suggests the transaction coordinator recited in these claims.

Further with respect to dependent claims 65, 66, 84, and 85, neither Shear nor Sudia suggests the integration of a trusted verifier module into another component as recited in these claims.

For the above reasons, the Examiner is requested to withdraw his rejection of claims 18-86; and to allow these claims as amended.

Applicant believes that this application is now in condition for allowance of all claims remaining herein, claims 1-14 and 18-86 as amended, and therefore an early Notice of Allowance is respectfully requested. If the Examiner disagrees or believes that for any other reason, direct contact with Applicant's attorney would help advance the prosecution of this case to finality, he is invited to telephone the undersigned at the number given below.

Respectfully submitted,

date of signature: July 25, 2006

Edward J. Radlo
Attorney Under Rule 34
Reg. No. 26,793

SONNENSCHEIN NATH & ROSENTHAL LLP
P.O. Box 061080
Wacker Drive Station, Sears Tower
Chicago, IL 60606-1080
Tel.: (415)882-2402

enclosures
cc: IP/T docket CH (w/encls.)
L. Miller (w/encls.) (via e-mail)
K. Ruthenberg (w/encls.)

27243613\V-2